PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-200519

(43)Date of publication of application : 31.07.1998

(51)Int.CI. H04L 9/08
H04L 9/10
H04L 9/12
H04L 12/54
H04L 12/58
H04M 11/00
H04N 1/44

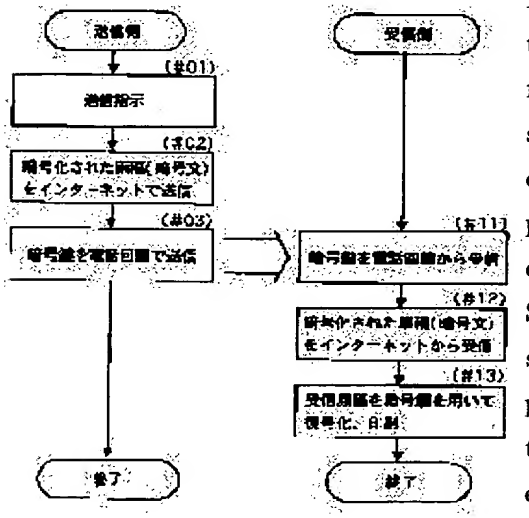
(21)Application number : 09-000230

(22)Date of filing : 06.01.1997

(71)Applicant : MURATA MACH LTD

(72)Inventor : YASUMOTO TADAYUKI

(54) COMMUNICATION TERMINAL DEVICE



(57)Abstract:

PROBLEM TO BE SOLVED: To communicate cipher text and a key of cryptogram through different routes for enhancing the confidentiality of communication by sending cipher text through a computer communication network and on the other hand, performing cipher communication that sends a key of cryptograph through a public line.

SOLUTION: A facsimile equipment on a sending end sends cipher text that is enciphered by an enciphering part through an internet (#02), when there is a transmission instruction with a start key operation, etc., (#01), and sends a key of a cryptograph that was used for encryption through a telephone line (#03). On the other hand, when a receiving end receives (#11) the key of the cryptogram through the telephone line, it automatically receives (#12) the cipher text through the internet, an enciphering part decodes it by using the key of cryptogram that receives the cipher text, and a recording part prints and outputs (#13) it. Here, when a key of the cryptogram is received through a telephone line, with this reception as a turning point, the receiving end automatically is connected to an internet and receives

the cipher text.

CLAIMS

[Claim(s)]

[Claim 1] The communication terminal which is a communication terminal which made connectable the computer communication network and the public line network, and is characterized by performing cryptocommunication by communicating a cryptographic key through the above-mentioned public line network while communicating a cipher through the above-mentioned computer communication network.

[Claim 2] The above-mentioned cryptographic key is a communication terminal according to claim 1 characterized by receiving by polling reception or confidential reception through the above-mentioned public line network.

[Claim 3] Claim 1 characterized by connecting the above-mentioned computer communication network automatically, and receiving the above-mentioned cipher when a cryptographic key is received through the above-mentioned public line network, or a communication terminal according to claim 2.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to amelioration of communication terminals, such as facsimile apparatus which enabled the communication link with a computer communication network.

[0002]

[Description of the Prior Art] Computer communication networks, such as the Internet, tend to be used increasingly, and those [its] who use also at ordinary homes are increasing in these days. Since only the communication link costs to a contract provider (provider to a computer communication network) nearby from a personal computer etc. in a user should pay use of such a computer communication network, it can shorten communication link time amount and has come to be also able to perform the communication link with an overseas computer by being cheap.

[0003] So, in current, in view of such a situation, communication terminals, such as facsimile apparatus which enabled connection with a computer communication network, are developed, and according to this, the manuscript image which carried out the reading scan can be transmitted now to a partner's communication terminal by either facsimile transmission or electronic mail transmission. That is, at the time of transmission of image data, when

facsimile transmission is chosen, image data is directly transmitted using a telephone network etc. On the other hand, when electronic mail transmission is chosen, image data was changed into the electronic mail format, this data was stored in the mail box on a network, and if many of receiving sides connect a computer communication network to the suitable tide via the telephone line by the dialup connection and the electronic mail is transmitted in this, image data is read from the mail box.

[0004] Although a lot of image data communication is possible with the spread of such equipment and communication networks, on the other hand, the cure against an information security has been a technical problem, and in order to solve this, cryptocommunication is used from the former.

[0005]

[Problem(s) to be Solved by the Invention] However, if cryptocommunication is performed through a computer communication network, the above-mentioned conventional communication terminal The cipher which enciphered the transmit data although the amount of data did not need to be extensive, or communication link cost did not need to start even if it was a long-distance communication link, Since it passed along various roots by the computer communication network without a change to transmit the cryptographic key (decode key) for decoding this cipher together, on the point [secreting nature, such as omission of the data in the middle of transmission, and tapping,], the problem still remained.

[0006] Then, this invention is communicating a cipher and a cryptographic key by another root in view of the above-mentioned situation, and it is proposed for the purpose of offering the communication terminal which raised communicative secreting nature further.

[0007]

[Means for Solving the Problem] While the communication terminal according to claim 1 proposed in order to attain the above-mentioned purpose is enabling connection of a computer communication network and a public line network and communicates a cipher through a computer communication network, it is characterized by performing cryptocommunication by communicating a cryptographic key through a public line network.

[0008] Although there are a cryptographic key of the narrow sense used in order to perform cipher processing, and a decode key used in order to perform decode processing in a cryptographic key here, in this invention, **** of a cryptographic key is mainly used by semantic **** of a decode key, and assumes the case where both are the same contents of data. However, you may be the contents from which these are different, and a decode key communicates through a public line network in that case.

[0009] In this communication terminal, while transmitting the cipher which performed cipher processing using the cryptographic key through a computer communication network at the time of transmission, a cryptographic key is transmitted through a public line network, and on the other hand, at the time of reception, after decoding the cipher received through the computer communication network by the cryptographic key which received through the public

line network, predetermined processing of a printout etc. is performed.

[0010] In addition, the facsimile apparatus with an electronic mail function made possible [connection of a computer communication network] for the communication terminal concerning this invention, the personal computer equipped with data communication facility, etc. are equivalent to this. Moreover, there are the Internet, NIFTY-Serve, PC-VAN which are personal computer communication service, etc. in a computer communication network, and electronic mail service is carried out as one of the services. There are a telephone network, ISDN (integrated services digital network), etc. in one public line network.

[0011] In a communication terminal according to claim 2, a cryptographic key receives by polling reception or confidential reception through a public line network. It is the function which is preventing from taking out the stored data here if polling reception is the function to receive the data which perform a Request to Send from a receiving side, and are set at the transmitting side, and confidential reception once stores the received data in memory and does not enter a predetermined password here.

[0012] When a cryptographic key is received through a public line network, a communication terminal according to claim 3 connects a computer communication network automatically, and receives a cipher. That is, reception of a cryptographic key shows that the cipher is already transmitted. Therefore, even if it is the case where the Internet is used by the dialup connection, this cipher is receivable immediately after a cipher is transmitted.

[0013]

[Embodiment of the Invention] Below, the gestalt of operation of this invention is explained with reference to a drawing. Drawing 1 is the block diagram showing an example of the internal configuration of the communication terminal of this invention. Here, the example of a configuration of the facsimile apparatus with an electronic mail function which is one of the communication terminals of this invention is shown. That is, in addition to conventional G3 and the facsimile communication facility of G4 which are performed through a public line network, this facsimile apparatus is equipped with the communication facility through a computer communication network, below, the Internet is used for a computer communication network, and electronic mail (e-mail) service is used and explained on the Internet.

[0014] CPU1 performs each processing of the encryption (decryption), and coding/decryption it not only controls each part of this facsimile apparatus, but mentioned later, image transformation, binary text conversion, e-mail edit, etc. through a bus 12. A read station 2 reads a manuscript by CCD etc., and outputs a monochrome binary image data. The Records Department 3 has printers, such as an electrophotography method, and records the image data which received through other G3 and G4 facsimile equipment to the Internet (printout). A display 4 is equipped with a liquid crystal display etc., and displays the operating state and image data of this facsimile apparatus. A control unit 5 is equipped with various keys, such as a ten key, a compaction dialing key, and an one-touch dialing key, and performs various input setup to this facsimile apparatus.

[0015] ROM6 memorizes software required for actuation of this facsimile apparatus. RAM7 memorizes temporary data generated at the time of activation of software, and also has memorized the various tables T1 mentioned later - T3. Image memory 8 consists of DRAMs etc. and memorizes an image data. DSU (Data Circuit Terminating Equipment: Digital Service Unit)9 performs conversion of a transmitted and received data and an electrical potential difference so that it can connect with the digital channel L1 which is using the base band transmission method. The modem 10 is equipped with the data modem function other than the conventional FAX modem function. NCU (network control unit: Network Control Unit)11 performs closing of an analog network L2, and disconnection.

[0016] Drawing 2 shows typically the data flow in the facsimile apparatus shown in drawing 1 . In this drawing, the same sign is given to drawing 1 and a corresponding part. Although the electronic mail transducer A mentioned later, a cryptopart 20, the coding decryption section 21, and the auto dialer 25 do not exist in drawing 1 , they shall be processed by CPU1 based on the software memorized by ROM6.

[0017] In addition, the electronic mail transducer A consists of the image transformation section 22, a binary text transducer 23, and the e-mail editorial department 24, and, in addition to facsimile communication, enables access to the Internet, and use of electronic mail service by equipping the conventional facsimile apparatus with this electronic mail transducer A. It enciphers using the cryptographic key which was able to be defined beforehand, or the image data (plaintext) read by the read station 2 is decrypted conversely, and a cryptopart 20 outputs it from the Records Department 3. In addition, there are DES (Data Encryption Standard), RSA, etc. in the method of encryption, and, specifically, it calculates multiplying this by the image data etc. using the predetermined bit string expressed in "1" as "0" to a cryptographic key. Hereafter, the image data enciphered in this way is called "encryption data."

[0018] The coding decryption section 21 encodes or decrypts encryption data with coding methods, such as MH, MR, and MMR. Hereafter, the data encoded by these coding methods are called "coded data." This coded data is memorized in image memory 8. In addition, although the case where encryption data are changed into coded data is shown, this invention is not limited to this, but you may make it encipher the encoded data, and a block with the cryptopart 20 in drawing 2 , and the coding decryption section 21 and image memory 8 interchanges in that case here.

[0019] At the time of transmission of an electronic mail, the image transformation section 22 changes it from TIFF at coded data at the time of reception, while changing coded data into TIFF (Tagged Image File format) which is the general graphics format used by computer. TIFF is various Class(es) which are exhibited by adobe and treat not only monochrome binary one but monochrome multiple value and full color **. It defines. Class F which treats a facsimile image to one of them It defines and is Class F to a head to coded data. If addition of TIFF header information etc. is performed, it is convertible for TIFF. The following and Class

F The coded data to which TIFF header information was added is called "TIFF data."

[0020] At the time of transmission of an electronic mail, while the binary text transducer 23 changes binary data into text data, it changes text data into binary data at the time of reception. Since the computer which cannot treat the electronic mail of binary data may be connected to the Internet, in order to make it an electronic mail arrive certainly to a phase hand, it is necessary to change binary data, such as TIFF data, into text data at the time of transmission.

[0021] In the document and RFC (Request For Comments)822 which IETF (Internet Engineering Task Fore) publishes, although specified as a 7-bit code, the text data treated by the Internet can change binary data into text data, if base64 of MIME (Multipurpose Internet Mail Extensions) etc. is used. In addition, it is the coding method which changes binary data into text data in base64 by considering that 8 bit x3 byte binary data are 6 bit x4 byte, and assigning a character code to each cutting tool.

[0022] While the e-mail editorial department 24 adds mail header information to the TIFF data changed into text data and edits into an electronic mail format, at the time of reception, mail header information is removed from the data of an electronic mail format at the time of transmission of an electronic mail, and it uses it as the TIFF data of text data. the head of the TIFF data which mail header information is the predetermined header information of the electronic mail of the Internet, and are transmitted here -- "From:", "To:", "Subject:", "cc:", and "Date: -- " etc. -- adding an item is specified.

[0023] The auto dialer 25 sends number-to-be-dialed data to DSU9, a modem 10, or NCU11 that automatic call origination of the number to be dialed read from the provider table T2 and phase hand table T3 should be carried out. Next, the configuration of each table T1 memorized by RAM7 - T3 is explained with drawing 3 .

[0024] The user ID for logging in to the Internet, a password, an e-mail address, and provider classification are registered into the user table T1 of drawing 3 (a) for every user who uses this facsimile apparatus. In addition, provider classification supports the provider classification of the provider table T2 of this drawing (b). The provider table T2 of this drawing (b) was made to correspond to provider classification, and a provider's number to be dialed (telephone number) used when accessing a provider name, a circuit class (an analog or digital), and the Internet is registered into it. By this, a different login procedure for every provider can be identified and performed, and when one user uses two or more providers, or even when the provider has two or more circuits, it can respond by setup of this table T2.

[0025] A phase hand name, an e-mail address, a facsimile number, and its classification (G3 or G4) are registered into phase hand table T3 of this drawing (c) for every abbreviated dialing number and one-touch number to be dialed. In addition, each table T1 - T3 can also carry out listing of the contents of a setting except the secret matter of a password etc. from the Records Department 3 or a display 4, then a setup of each table T1 by the user, a manager, etc. - T3, modification, and a check become simple.

[0026] By the above configurations, this facsimile apparatus performs cryptocommunication which raised secreting nature more compared with the former. An outline flow shows an example of the actuation at this time to drawing 4 . In the facsimile apparatus of a transmitting side, by actuation of a start key etc., if there are transmitting directions, the manuscript data (cipher) enciphered by the cryptopart 20 will be transmitted by the Internet, and the cryptographic key used by encryption will be transmitted through the telephone lines L1 and L2 (#01-#03).

[0027] On the other hand, in a receiving side, if a cryptographic key is received through the telephone lines L1 and L2, a cipher will be automatically received through the Internet, it will decrypt in a cryptopart 20 using the cryptographic key which received the cipher, and a printout (printing) will be carried out from the Records Department 3 (#11-#13). Here, when a cryptographic key is received through the telephone lines L1 and L2 which are public line networks, this became an opportunity, connected automatically the Internet which is a computer communication network, and has received the cipher. By this, if a cryptographic key is received even if it is the case where the Internet is used with a dial-up connection type, it turns out that the cipher is already transmitted and quick data transmission can be realized.

[0028] In addition, a cryptographic key communicates by communicating by the junction multiple address indication signal which is sent and received by facsimile communication and to which multiple address transmission is made to carry out from a relay center, and the new signal of the same kind, or including in NSF in a communication procedure (non-standard functional recognition signal) etc. as a new item conventionally. Next, the configuration of the communication network equipped with the above-mentioned facsimile apparatus is shown in drawing 5 . Here, although F in drawing explains that actuation below as a thing applicable to this facsimile apparatus with an electronic mail function, the personal computer PC connected by the dedicated line is sufficient as the communication terminal of this invention, and even if it does not perform a dialup connection to the tide of periodical or arbitration, according to this, it can carry out data communication to real time.

[0029] When performing cryptocommunication from facsimile apparatus F to a phase hand's facsimile apparatus Fa with an electronic mail function and personal computer PCa, first, in advance of transmission of a cryptographic key, that a cipher should be transmitted by E-mail, a contract provider is called through the public line network P, computer communication network N is connected and the image data which carried out the reading scan is transmitted (root **-**).

[0030] Then, a cryptographic key is transmitted through the public line networks P and Pa (root **-**-**, **-**-**). Since the cipher is already transmitted to a phase hand's facsimile apparatus Fa, and addressing to Computer PCa by E-mail, computer communication network N can be connected to the tide of reception and coincidence of a cryptographic key, or subsequent arbitration through the public line network Pa, the electronic mail addressed to the self-address can be received (root **-**, **-**), and a cipher can be decrypted.

[0031] If it communicates in such a gestalt, since the cipher with much amount of data will be sent and received through computer communication network N, on the both sides of a transmitting side F and receiving sides Fa and PCa, much traffic does not start like [at the time of sending and receiving a cipher] by the usual facsimile communication (root **-**-**, **-**-**, **-**-**) that what is necessary is just to pay the traffic to a contract provider. In addition, Fb in drawing is the usual facsimile apparatus which is not equipped with the electronic mail function.

[0032] Moreover, since Computer PC was connected to computer communication network N by the leased connection and other networks Na are connected to it by LAN connection etc., an electronic mail can also be transmitted to the computer PC of a leased connection, and the network Na of LAN connection from facsimile apparatus F (root **-**-**, **-**-**). In addition, if the public line networks P and Pa are connected to Computer PC and Network Na also in this case, the same cryptocommunication as the above can be performed.

[0033] Next, the basic actuation at the time of reception of the communication terminal (facsimile apparatus with an electronic mail function) of this invention is explained with the flow chart of drawing 6 . Here, if confidential reception of the cryptographic key is carried out through the public line networks P and Pa (steps 100-106) and reception of this cryptographic key is checked first, by the dialup connection, the Internet is accessed and the case (steps 107-121) where a cipher is received is shown.

[0034] If a message is received to the call confidential transmission was instructed to be, the data of the cryptographic key which received will be memorized in the confidential box (RAM7) specified from the transmitting side. And a circuit is opened wide and it displays having carried out confidential reception on record or a display 4 by the Records Department 3 with the destination, a confidential box number, etc. Then, if the personal identification number (password) corresponding to a confidential box is inputted, it will display that it is cryptocommunication on record or a display 4 by the Records Department 3 so that only the person who inputted this personal identification number may understand (above, steps 100-106).

[0035] Next, the person who checked cryptocommunication chooses data, such as self user ID, from the user table T1 by actuation of a control unit 5 etc. first that the cipher which is the text should be received. Then, if the circuit class of the provider who connects is read from the provider table T2, DSU9 will be set up if it is an analog network and is a setup and a digital channel about a modem 10, call origination of a provider's telephone number is carried out and there is arrival of the mail, reception of an electronic mail (cipher) will be started.

[0036] To a protocol, reception of an electronic mail logs in using PAP (Password Authentication Protocol), and receives data by POP (Post Office Protocol) here. Then, from the data of the received electronic mail, after removing an electronic mail header by the e-mail editorial department 24, changing this into binary data by the binary text transducer 23, returning to coded data from TIFF data by the image transformation section 22 and

decrypting coded data by the coding decryption section 21, this data is decoded by the cryptopart 20 using the cryptographic key which is confidential reception ending. This decoded image data is displayed on record or a display 4 by the Records Department 2, and a circuit is opened wide after that (above, steps 107-121).

[0037] Although the case where confidential reception received a cryptographic key was shown above, in this invention, it is also receivable with polling reception (Request-to-Send reception) in addition to this. Polling reception performs a Request to Send from a receiving side to the communication terminal (transmitting side) defined beforehand by actuation of a control unit 5, or time-of-day assignment, and receives the data set to the transmitting side (it memorizes in memory). According to this, a cryptographic key can be received to the favorite tide after receiving a cipher through computer communication network N, and decode (decode) of a cipher can be started.

[0038] In addition, this invention can also take the gestalt of operations other than the above, and may often (for example, WWW of the Internet) also as data, such as voice and an animation, use computer communication networks other than the Internet (for example, NIFTY-Serve) for transmission of an electronic mail for the data transmitted in computer communication network N in addition to an image data.

[0039]

[Effect of the Invention] Since communication link cost can be made cheap by leaps and bounds since a cipher is communicated through a computer communication network and a cryptographic key is communicated through the public line network whose cipher is another root when performing cryptocommunication according to the communication terminal of this invention according to claim 1 so that he can understand also from the above explanation, compared with the former, communicative secreting nature increases further.

[0040] According to the communication terminal according to claim 2, since polling reception or confidential reception receives a cryptographic key, the communication link holding a secret is attained further. According to the communication terminal according to claim 3, by reception of a cryptographic key, it can judge that the cipher is already transmitted, a computer communication network can be connected automatically, and a cipher can be received. Therefore, even when using a computer communication network by the dialup connection, data transmission can be done quickly.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is the block diagram having shown an example of the internal configuration of the communication terminal concerning this invention.

[Drawing 2] It is the mimetic diagram having shown the data flow in the communication terminal concerning this invention.

[Drawing 3] It is drawing having shown an example of the configuration of the table memorized by the communication terminal concerning this invention.

[Drawing 4] It is the flow chart which shows an outline for actuation of the communication terminal concerning this invention.

[Drawing 5] It is drawing having shown an example of the configuration of the communication network equipped with the communication terminal concerning this invention.

[Drawing 6] It is the flow chart which shows an example of the basic actuation at the time of reception of the communication terminal concerning this invention.

[Description of Notations]

20 ... Cryptopart

A ... Electronic mail transducer

N ... Computer communication network

P, Pa ... Public line network

F ... Facsimile apparatus with an electronic mail function

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－200519

(43)公開日　平成10年(1998)７月31日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ｂ
9/10		Ｈ０４Ｍ　11/00	３０３
9/12		Ｈ０４Ｎ　1/44	
12/54		Ｈ０４Ｌ　9/00	６２１Ａ
12/58			６３１

審査請求　未請求　請求項の数３　ＯＬ　（全 10 頁）　最終頁に続く

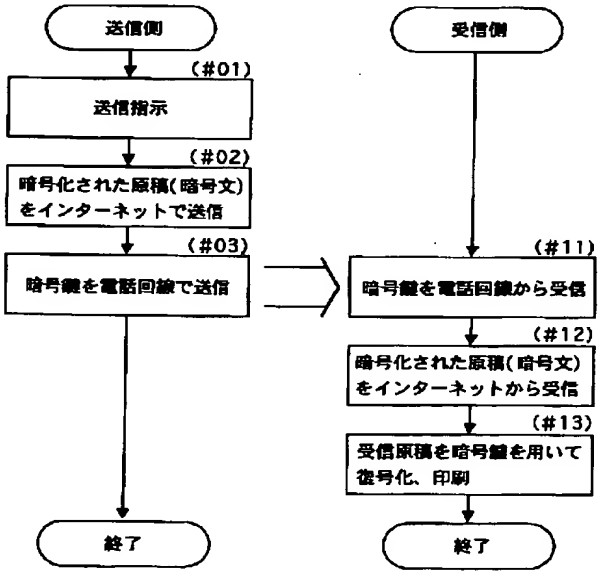
(21)出願番号　特願平9－230

(22)出願日　平成９年(1997)１月６日

(71)出願人　000006297
村田機械株式会社
京都府京都市南区吉祥院南落合町３番地
(72)発明者　安本　格之
京都市伏見区竹田向代町136番地　村田機械株式会社本社工場内
(74)代理人　弁理士　中井　宏行

(54)【発明の名称】　通信端末装置

(57)【要約】
【課題】暗号文と暗号鍵を別のルートで通信することで、通信の秘守性を更に高めた通信端末装置を提供する。
【解決手段】本発明に係る通信端末装置は、コンピュータ通信網と公衆回線網とを接続可能として、コンピュータ通信網を介して暗号文を通信（＃０２，＃１２）する一方、公衆回線網を介して暗号鍵を通信（＃０３，＃１１）することによって、暗号通信を行うことを特徴とする。



【特許請求の範囲】
【請求項１】コンピュータ通信網と公衆回線網とを接続可能とした通信端末装置であって、
上記コンピュータ通信網を介して暗号文を通信する一方、上記公衆回線網を介して暗号鍵を通信することによって、暗号通信を行うことを特徴とする通信端末装置。
【請求項２】上記暗号鍵は、上記公衆回線網を介して、ポーリング受信あるいは親展受信によって受信することを特徴とする請求項１に記載の通信端末装置。
【請求項３】上記公衆回線網を介して暗号鍵を受信したときには、上記コンピュータ通信網を自動的に接続し、上記暗号文を受信することを特徴とする請求項１あるいは請求項２に記載の通信端末装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、コンピュータ通信網との通信を可能としたファクシミリ装置等の通信端末装置の改良に関する。
【０００２】
【従来の技術】インターネット等のコンピュータ通信網は益々利用される傾向にあり、近頃では、一般家庭においても利用する人が増えている。このようなコンピュータ通信網の利用は、利用者がパーソナルコンピュータなどから、最寄りの契約プロバイダ（コンピュータ通信網への接続業者）までの通信費用のみの負担するだけでよいため、通信時間が短縮でき、海外のコンピュータとの通信も安価でできるようになっている。
【０００３】そこで現在では、このような状況を鑑みて、コンピュータ通信網への接続を可能としたファクシミリ装置などの通信端末装置が開発されており、これによれば、読取走査した原稿画像を、ファクシミリ送信、あるいは、電子メール送信のいずれかによって、相手の通信端末装置に送信できるようになっている。即ち、画像データの送信時に、ファクシミリ送信を選択したときには、電話網などを使用して直接、画像データを送信する。一方、電子メール送信を選択したときには、画像データを電子メール形式に変換し、このデータをネットワーク上のメールボックスに格納して、これを受信側の多くが、ダイヤルアップ接続によって、適当な時機に電話回線経由でコンピュータ通信網を接続し、電子メールが送信されていれば、メールボックスから画像データを読み出している。
【０００４】このような装置及び通信網の普及に伴って、大量の画像データ通信が可能になっているが、その一方では、情報セキュリティ対策が課題になっており、これを解決するため、従来から暗号通信が利用されている。
【０００５】
【発明が解決しようとする課題】ところが、上記従来の通信端末装置は、暗号通信をコンピュータ通信網を通じて行えば、データ量が大量であったり長距離通信であっても、通信コストがかからずに済むが、送信データを暗号化した暗号文と、この暗号文を復号するための暗号鍵（復号鍵）とを一緒に送信することには変わりなく、また、コンピュータ通信網では、様々なルートを通るため、依然、伝送途中でのデータの遺漏、盗聴などの秘守性の点では、問題が残っていた。
【０００６】そこで、本発明は上記事情に鑑みて、暗号文と暗号鍵を別のルートで通信することで、通信の秘守性を更に高めた通信端末装置を提供することを目的として提案される。
【０００７】
【課題を解決するための手段】上記目的を達成するために提案される請求項１に記載の通信端末装置は、コンピュータ通信網と公衆回線網とを接続可能としており、コンピュータ通信網を介して暗号文を通信する一方、公衆回線網を介して暗号鍵を通信することによって、暗号通信を行うことを特徴とする。
【０００８】ここに暗号鍵には、暗号処理を行うために用いる狭義の暗号鍵と、復号処理を行うために用いる復号鍵とがあるが、本発明においては、暗号鍵の文言は、主に復号鍵の意味あいで用いており、両者が同じデータ内容である場合を想定している。但し、これらが違う内容であってもよく、その場合は、復号鍵が公衆回線網を通じて通信される。
【０００９】この通信端末装置では、送信時は、暗号鍵を用いて暗号処理を行った暗号文を、コンピュータ通信網を通じて送信するとともに、暗号鍵を公衆回線網を通じて送信し、一方、受信時は、コンピュータ通信網を通じて受信した暗号文を、公衆回線網を通じて受信した暗号鍵によって復号した後に、印字出力などの所定の処理を行う。
【００１０】なお、本発明に係る通信端末装置は、コンピュータ通信網を接続可能とした電子メール機能付きファクシミリ装置や、データ通信機能を備えたパーソナルコンピュータ等がこれに相当する。また、コンピュータ通信網には、インターネットや、パソコン通信サービスであるＮＩＦＴＹ－Ｓｅｒｖｅ、ＰＣ－ＶＡＮなどがあり、サービスの１つとして電子メールサービスを実施している。一方の公衆回線網には、電話網、ＩＳＤＮ（サービス総合デジタル網）などがある。
【００１１】請求項２に記載の通信端末装置では、暗号鍵は、公衆回線網を介して、ポーリング受信あるいは親展受信によって受信する。ここに、ポーリング受信とは、受信側から送信要求を行って、送信側にセットされているデータを受信する機能であり、親展受信とは、受信したデータを一旦メモリに蓄積し、所定のパスワードを入力しなければ、蓄積しているデータを取り出すことができないようにしている機能である。
【００１２】請求項３に記載の通信端末装置は、公衆回

線網を介して暗号鍵を受信したときには、コンピュータ通信網を自動的に接続し暗号文を受信する。即ち、暗号鍵の受信によって、暗号文が既に送信されていることが分かる。したがって、インターネットをダイヤルアップ接続で利用する場合であっても、暗号文が送信された後すぐに、この暗号文を受信することができる。

【００１３】

【発明の実施の形態】以下に、図面を参照して本発明の実施の形態を説明する。図１は、本発明の通信端末装置の内部構成の一例を示すブロック図である。ここでは、本発明の通信端末装置の１つである電子メール機能付ファクシミリ装置の構成例を示す。即ち、このファクシミリ装置には、公衆回線網を介して行う従来のＧ３，Ｇ４のファクシミリ通信機能に加えて、コンピュータ通信網を介した通信機能を備えており、以下には、コンピュータ通信網にインターネットを使用し、インターネット上で電子メール（ｅ－ｍａｉｌ）サービスを利用する説明する。

【００１４】ＣＰＵ１は、バス１２を通じて、このファクシミリ装置の各部を制御するだけではなく、後述する暗号化（復号化）、符号化／復号化、画像変換、バイナリ・テキスト変換、メール編集などの各処理を実行する。読取部２は、ＣＣＤ等で原稿を読み取り、白黒２値のイメージデータを出力する。記録部３は、電子写真方式などのプリンタを備え、他のＧ３，Ｇ４ファクシミリ装置から、あるいはインターネットを介して、受信したイメージデータを記録（印字出力）する。表示部４は、液晶表示装置などを備え、このファクシミリ装置の動作状態やイメージデータを表示する。操作部５はテンキー、短縮ダイヤルキー、ワンタッチダイヤルキーなどの各種キーを備えて、このファクシミリ装置に対し、各種入力設定を行う。

【００１５】ＲＯＭ６は、このファクシミリ装置の動作に必要なソフトウェアを記憶する。ＲＡＭ７は、ソフトウェアの実行時に発生する一時的なデータを記憶するほか、後述する各種テーブルＴ１～Ｔ３を記憶している。イメージメモリ８は、ＤＲＡＭ等で構成され、イメージデータを記憶する。ＤＳＵ（データ回線終端装置：Digital Service Unit）９は、ベースバンド伝送方式を使用しているデジタル回線Ｌ１に接続できるように、送受信データと電圧の変換を行う。モデム１０は、従来のＦＡＸモデム機能の他にデータモデム機能を備えている。ＮＣＵ（網制御装置：Network Control Unit）１１は、アナログ回線Ｌ２の閉結、開放を行う。

【００１６】図２は、図１に示したファクシミリ装置内のデータの流れを模式的に示したものである。この図では、図１と対応する箇所には同じ符号を付している。後述する電子メール変換部Ａ、暗号部２０、符号化復号化部２１、オートダイヤラー２５は、図１には存在しないが、ＲＯＭ６に記憶されたソフトウェアに基づいて、ＣＰＵ１によって処理されるものとする。

【００１７】なお、電子メール変換部Ａは、画像変換部２２、バイナリ・テキスト変換部２３、メール編集部２４で構成されており、従来のファクシミリ装置に、この電子メール変換部Ａを備えることによって、ファクシミリ通信に加え、インターネットへのアクセス、及び電子メールサービスの利用を可能にしている。暗号部２０は、読取部２で読み取ったイメージデータ（平文）を、予め定められた暗号鍵を用いて暗号化し、あるいは、逆に復号化して記録部３から出力する。なお、暗号化の方式には、ＤＥＳ（Data Encryption Standard）やＲＳＡなどがあり、具体的には、例えば、暗号鍵に「０」と「１」とで表される所定のビット列を用い、これをイメージデータと掛け合わせるなどの演算を行う。以下、このように暗号化されたイメージデータを「暗号化データ」と呼ぶ。

【００１８】符号化復号化部２１は、暗号化データをＭＨ，ＭＲ，ＭＭＲ等の符号化方式によって符号化または復号化する。以下、これらの符号化方式によって符号化されたデータを「符号化データ」と呼ぶ。イメージメモリ８には、この符号化データを記憶する。なお、ここでは、暗号化データを符号化データに変換する場合を示しているが、本発明はこれには限定されず、符号化したデータを暗号化するようにしてもよく、その場合は、図２における暗号部２０と、符号化復号化部２１及びイメージメモリ８とのブロックが入れ替わる。

【００１９】画像変換部２２は、電子メールの送信時に、符号化データを、コンピュータで使用される一般的な画像フォーマットである、ＴＩＦＦ（Tagged Image File format）に変換する一方、受信時には、ＴＩＦＦから符号化データに変換する。ＴＩＦＦは、ａｄｏｂｅ社によって公開されており、白黒２値だけではなく、白黒多値、フルカラーなどを扱う様々なClass が定義されている。その中の１つには、ファクシミリ画像を扱うClass Ｆ が定義されており、符号化データに対して、先頭にClass Ｆ のＴＩＦＦヘッダ情報の付加などを行えば、ＴＩＦＦに変換できる。以下、Class Ｆ のＴＩＦＦヘッダ情報が付加された符号化データを「ＴＩＦＦデータ」と呼ぶ。

【００２０】バイナリ・テキスト変換部２３は、電子メールの送信時は、バイナリデータをテキストデータに変換する一方、受信時には、テキストデータをバイナリデータに変換する。インターネットには、バイナリデータの電子メールを扱うことが出来ないコンピュータを接続している場合があるので、相手先に対し確実に電子メールが届くようにするには、ＴＩＦＦデータなどのバイナリデータは、送信時にテキストデータに変換する必要がある。

【００２１】インターネットで扱うテキストデータは、ＩＥＴＦ（Internet Engineering Task Fore）が発行す

るドキュメント、ＲＦＣ（Request For Comments）８２２において、７ビットのコードとして規定されているが、ＭＩＭＥ（Multipurpose Internet Mail Extensions）のｂａｓｅ６４などを利用すれば、バイナリデータをテキストデータに変換できる。なお、ｂａｓｅ６４とは、８ビット×３バイトのバイナリデータを６ビット×４バイトと見なし、各々のバイトに対し、キャラクタコードを割り当てることにより、バイナリデータをテキストデータに変換する符号化方式である。

【００２２】メール編集部２４は、電子メールの送信時は、テキストデータに変換されたＴＩＦＦデータにメールヘッダ情報を付加して電子メール形式に編集する一方、受信時には、電子メール形式のデータからメールヘッダ情報を取り除き、テキストデータのＴＩＦＦデータとする。ここに、メールヘッダ情報とは、インターネットの電子メールの所定のヘッダ情報のことであり、送信するＴＩＦＦデータの先頭に、"From:"，"To:"，"Subject:"，"cc:"，"Date:" などの項目を付加することが規定されている。

【００２３】オートダイヤラー２５は、プロバイダテーブルＴ２、相手先テーブルＴ３から読み出したダイヤル番号を自動発呼すべく、ＤＳＵ９、モデム１０またはＮＣＵ１１へダイヤル番号データを送る。次に、ＲＡＭ７に記憶された各テーブルＴ１～Ｔ３の構成について図３とともに説明する。

【００２４】図３（ａ）の利用者テーブルＴ１には、このファクシミリ装置を使用するユーザ毎に、インターネットにログインするためのユーザＩＤとパスワード、電子メールアドレス、プロバイダ種別を登録している。なお、プロバイダ種別は同図（ｂ）のプロバイダテーブルＴ２のプロバイダ種別に対応している。同図（ｂ）のプロバイダテーブルＴ２には、プロバイダ種別に対応させて、プロバイダ名称、回線種別（アナログまたはデジタル）、インターネットに接続するときに使用するプロバイダのダイヤル番号（電話番号）を登録している。これによって、プロバイダ毎に異なるログイン手順を識別して実行することができ、１人のユーザが複数のプロバイダを利用する場合や、プロバイダが複数の回線を有している場合でも、このテーブルＴ２の設定によって対応できる。

【００２５】同図（ｃ）の相手先テーブルＴ３には、短縮ダイヤル番号、ワンタッチダイヤル番号毎に、相手先名称、電子メールアドレス、ファクシミリ番号とその種別（Ｇ３またはＧ４）を登録している。なお、各テーブルＴ１～Ｔ３は、パスワードなどの秘密事項を除く設定内容を、記録部３や表示部４からリスト出力することもでき、そうすれば、ユーザや管理者などによる各テーブルＴ１～Ｔ３の設定、変更、確認作業が簡易になる。

【００２６】以上のような構成によって、このファクシミリ装置は、従来と比べ、より秘守性を高めた暗号通信を行う。このときの動作の一例を概略フローで図４に示す。送信側のファクシミリ装置では、スタートキーの操作などにより、送信指示があると、暗号部２０で暗号化された原稿データ（暗号文）をインターネットで送信し、暗号化で使用した暗号鍵を電話回線Ｌ１，Ｌ２を通じて送信する（＃０１～＃０３）。

【００２７】一方、受信側では、電話回線Ｌ１，Ｌ２を介して暗号鍵を受信すると、自動的にインターネットを通じて暗号文を受信し、暗号部２０において、暗号文を受信した暗号鍵を用いて復号化し、記録部３から印字出力（印刷）する（＃１１～＃１３）。ここでは、公衆回線網である電話回線Ｌ１，Ｌ２を介して、暗号鍵を受信したときに、これが契機となって、コンピュータ通信網であるインターネットを自動的に接続して、暗号文を受信している。これによって、ダイヤルアップ接続方式によってインターネットを利用する場合であっても、暗号鍵を受信すれば、既に暗号文が送信されていることが分かり、迅速なデータ伝送が実現できる。

【００２８】なお、暗号鍵は、従来、ファクシミリ通信で送受されている、中継局から同報送信を行わせる中継同報指示信号などと同種の新規な信号で通信され、あるいは、通信手順内のＮＳＦ（非標準機能識別信号）などに新たな項目として含めることによって通信される。次に、上記ファクシミリ装置を備えた通信網の構成を図５に示す。ここでは、図中のＦがこの電子メール機能付ファクシミリ装置に該当するものとして、以下にその動作を説明するが、本発明の通信端末装置は、専用線で接続されたパーソナルコンピュータＰＣでもよく、これによれば、定期的あるいは任意の時機にダイヤルアップ接続を行わなくても、リアルタイムにデータ通信を行うことができる。

【００２９】ファクシミリ装置Ｆから、相手先の電子メール機能付ファクシミリ装置Ｆａやパーソナルコンピュータ ＰＣａに対し、暗号通信を行うときには、まず、暗号鍵の送信に先だって、暗号文を電子メールで送信すべく、公衆回線網Ｐを介して契約プロバイダを呼び出し、コンピュータ通信網Ｎを接続し、読取走査した画像データを送信する（ルート①～②）。

【００３０】続いて、暗号鍵を、公衆回線網Ｐ，Ｐａを介して送信する（ルート①～④～⑤，①～④～⑥）。相手先のファクシミリ装置Ｆａ、コンピュータＰＣａ宛に、すでに暗号文を電子メールで送信しているので、暗号鍵の受信と同時、あるいは、その後の任意の時機に、公衆回線網Ｐａを介してコンピュータ通信網Ｎを接続し、自アドレス宛の電子メールを受信して（ルート⑤～③，⑥～③）、暗号文を復号化することができる。

【００３１】このような形態において通信すれば、データ量が多い暗号文はコンピュータ通信網Ｎを通じて送受されるので、送信側Ｆ、受信側Ｆａ，ＰＣａの双方では、契約プロバイダまでの通信費を支払うだけでよく、

通常のファクシミリ通信（ルート①～④～⑤，①～④～⑥，①～④～⑦）によって、暗号文を送受した場合のように、多くの通信費がかかることがない。なお、図中のＦｂは、電子メール機能を備えていない通常のファクシミリ装置である。

【００３２】また、コンピュータ通信網Ｎには、専用線接続によってコンピュータＰＣを接続し、ＬＡＮ接続などによって他のネットワークＮａも接続しているので、ファクシミリ装置Ｆから、専用線接続のコンピュータＰＣ、ＬＡＮ接続のネットワークＮａに電子メールを送信することもできる（ルート①～②～⑧，①～②～⑨）。なお、この場合も、コンピュータＰＣ、ネットワークＮａに公衆回線網Ｐ，Ｐａを接続していれば、上記と同様の暗号通信ができる。

【００３３】次に、本発明の通信端末装置（電子メール機能付ファクシミリ装置）の受信時の基本動作について、図６のフローチャートとともに説明する。ここでは、まず、暗号鍵を公衆回線網Ｐ，Ｐａを介して親展受信し（ステップ１００～１０６）、この暗号鍵の受信を確認すれば、ダイヤルアップ接続によって、インターネットにアクセスし、暗号文を受信する（ステップ１０７～１２１）場合を示している。

【００３４】親展送信が指示された呼出に対して着信すると、受信した暗号鍵のデータを、送信側から指定された親展ボックス（ＲＡＭ７）に記憶する。そして、回線を開放し、親展受信したことを、宛先や親展ボックス番号などとともに、記録部３によって記録、あるいは、表示部４に表示する。その後、親展ボックスに対応した暗証番号（パスワード）が入力されれば、この暗証番号を入力した人だけに分かるように、暗号通信であることを、記録部３によって記録、あるいは、表示部４に表示する（以上、ステップ１００～１０６）。

【００３５】次に、暗号通信を確認した人は、本文である暗号文を受信すべく、まず、操作部５の操作などによって、利用者テーブルＴ１から自己のユーザＩＤなどのデータを選択する。すると、プロバイダテーブルＴ２から、接続するプロバイダの回線種別を読み出し、アナログ回線であればモデム１０を設定、デジタル回線であればＤＳＵ９を設定して、プロバイダの電話番号を発呼し、着信があれば、電子メール（暗号文）の受信を開始する。

【００３６】ここに、電子メールの受信は、プロトコルに、例えば、ＰＡＰ（Password Authentication Protocol）を使用してログインし、ＰＯＰ（Post Office Protocol）によりデータを受信する。続いて、受信した電子メールのデータから、メール編集部２４によって電子メールヘッダを取り除き、これをバイナリ・テキスト変換部２３でバイナリデータに変換し、画像変換部２２によってＴＩＦＦデータから符号化データに戻し、符号化復号化部２１によって符号化データを復号化した後、暗号部２０によって、このデータを親展受信済みである暗号鍵を用いて復号する。この復号したイメージデータは、記録部２によって記録、あるいは、表示部４に表示され、その後、回線が開放される（以上、ステップ１０７～１２１）。

【００３７】以上には、暗号鍵を親展受信によって受信する場合を示したが、本発明では、これ以外に、ポーリング受信（送信要求受信）によって受信することもできる。ポーリング受信とは、操作部５の操作、あるいは、時刻指定によって、予め定められた通信端末装置（送信側）に対し、受信側から送信要求を行って、送信側にセット（メモリに記憶）されているデータを受信するものである。これによれば、コンピュータ通信網Ｎを介して暗号文を受信した後の好きな時機に暗号鍵を受信し、暗号文の復号（解読）を開始することができる。

【００３８】なお、本発明は、上記以外の実施の形態をとることもでき、コンピュータ通信網Ｎにおいて送信するデータを、イメージデータ以外に、音声、動画などのデータとしてもよく（例えば、インターネットのＷＷＷ）、電子メールの送信に、インターネット以外のコンピュータ通信網（例えば、ＮＩＦＴＹ－Ｓｅｒｖｅ）を使用してもよい。

【００３９】

【発明の効果】以上の説明からも理解できるように、本発明の請求項１に記載の通信端末装置によれば、暗号通信を行うときに、暗号文をコンピュータ通信網を介して通信するので通信コストを飛躍的に安価にすることが出来、また、暗号鍵を、暗号文とは別ルートである公衆回線網を介して通信するので、従来と比べ、通信の秘守性が更に高まる。

【００４０】請求項２に記載の通信端末装置によれば、暗号鍵を、ポーリング受信あるいは親展受信によって受信するので、更に、秘密を保持した通信が可能になる。請求項３に記載の通信端末装置によれば、暗号鍵の受信によって、暗号文が既に送信されていることが判断でき、自動的にコンピュータ通信網を接続し暗号文を受信することができる。したがって、コンピュータ通信網をダイヤルアップ接続によって利用する場合でも、迅速にデータ伝送ができる。

【図面の簡単な説明】

【図１】本発明に係る通信端末装置の内部構成の一例を示したブロック図である。

【図２】本発明に係る通信端末装置内のデータの流れを示した模式図である。

【図３】本発明に係る通信端末装置に記憶されるテーブルの構成の一例を示した図である。

【図４】本発明に係る通信端末装置の動作を概略を示すフローチャートである。

【図５】本発明に係る通信端末装置を備えた通信網の構成の一例を示した図である。

【図６】本発明に係る通信端末装置の受信時の基本動作の一例を示すフローチャートである。

【符号の説明】

２０・・・暗号部

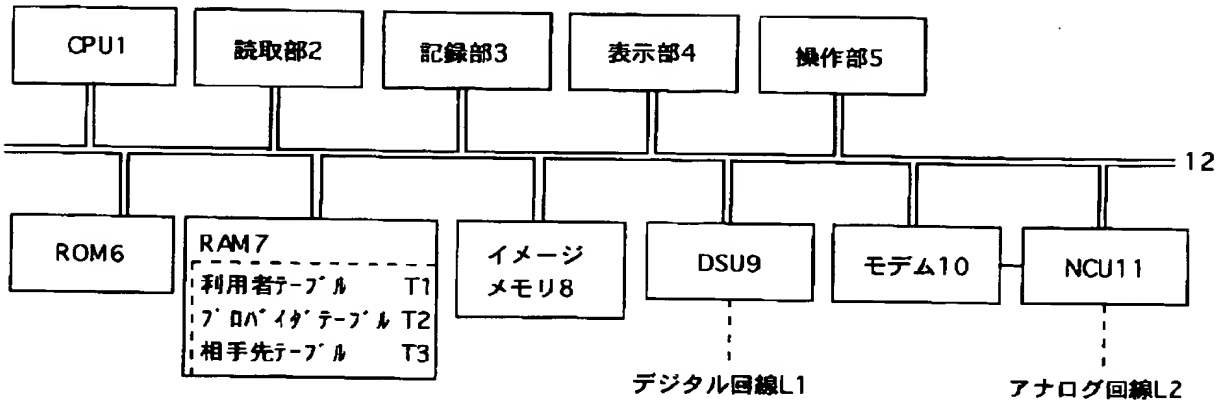
Ａ・・・電子メール変換部

Ｎ・・・コンピュータ通信網

Ｐ，Ｐａ・・・公衆回線網

Ｆ・・・電子メール機能付ファクシミリ装置

【図１】



【図３】

(a) 利用者テーブルT1

ﾕｰｻﾞ名	ﾕｰｻﾞID	ﾊﾟｽﾜｰﾄﾞ	電子ﾒｰﾙｱﾄﾞﾚｽ	ﾌﾟﾛﾊﾞｲﾀﾞ種別
○○○○	maru	abcd	maru@kyoto.co.jp	A
××××	batsu	xyz	batsu@osaka.or.jp	B

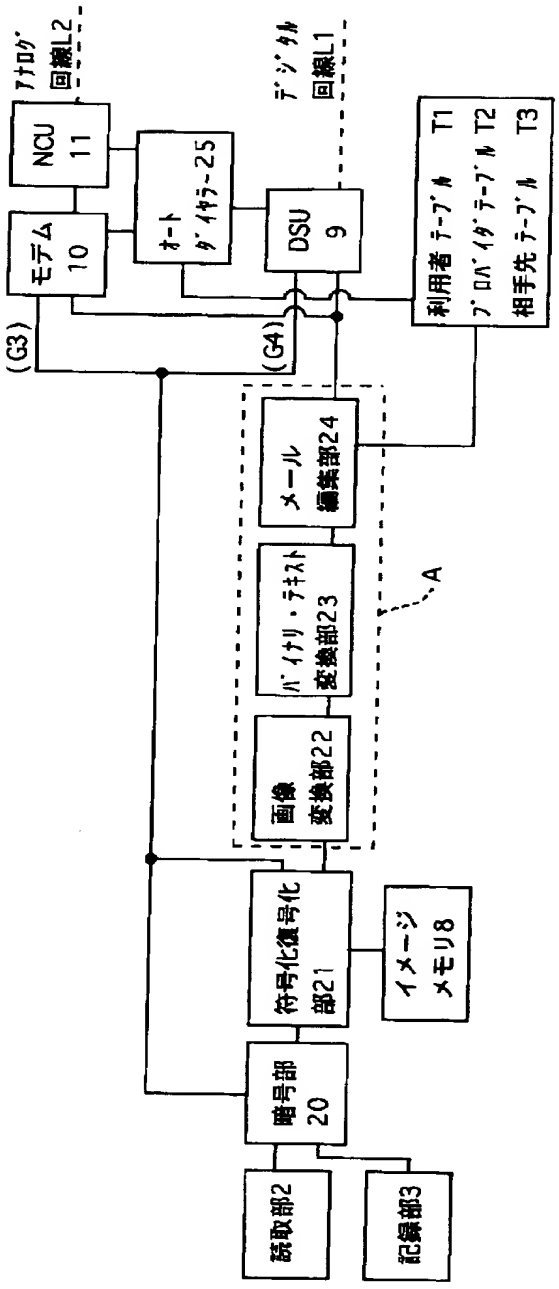
(b)プロバイダテーブルT2

ﾌﾟﾛﾊﾞｲﾀﾞ種別	ﾌﾟﾛﾊﾞｲﾀﾞ名称	回線種別	電話番号
A	○○ネット	デジタル	075-222-7777
B	××ネット	アナログ	06-123-4567

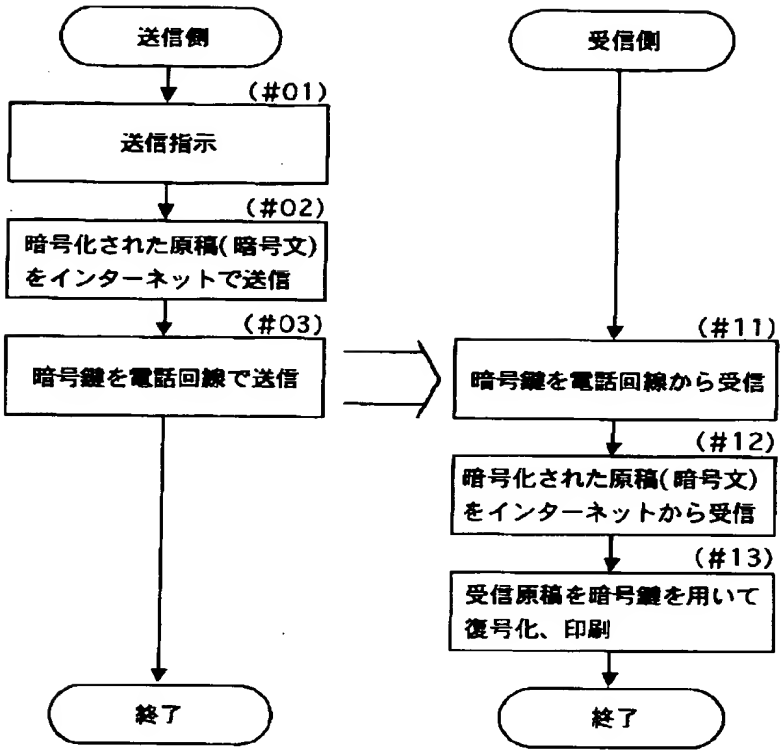
(c)相手先テーブルT3

短縮/ﾜﾝﾀｯﾁ	相手先名称	電子ﾒｰﾙｱﾄﾞﾚｽ	ﾌｧｸｼﾐﾘ番号	ﾌｧｸｼﾐﾘ種別
短縮001	ABC㈱	abc@abc.co.jp	075-123-4567	G4
短縮002	㈱efg	efg@kyoto.or.jp	075-321-1111	G3
ﾜﾝﾀｯﾁA	xyz商会	xyz00123@niftyserve.or.jp	06-789-2222	G3
ﾜﾝﾀｯﾁB	××商店	hijk@kyoto.or.jp	075-345-3333	G4

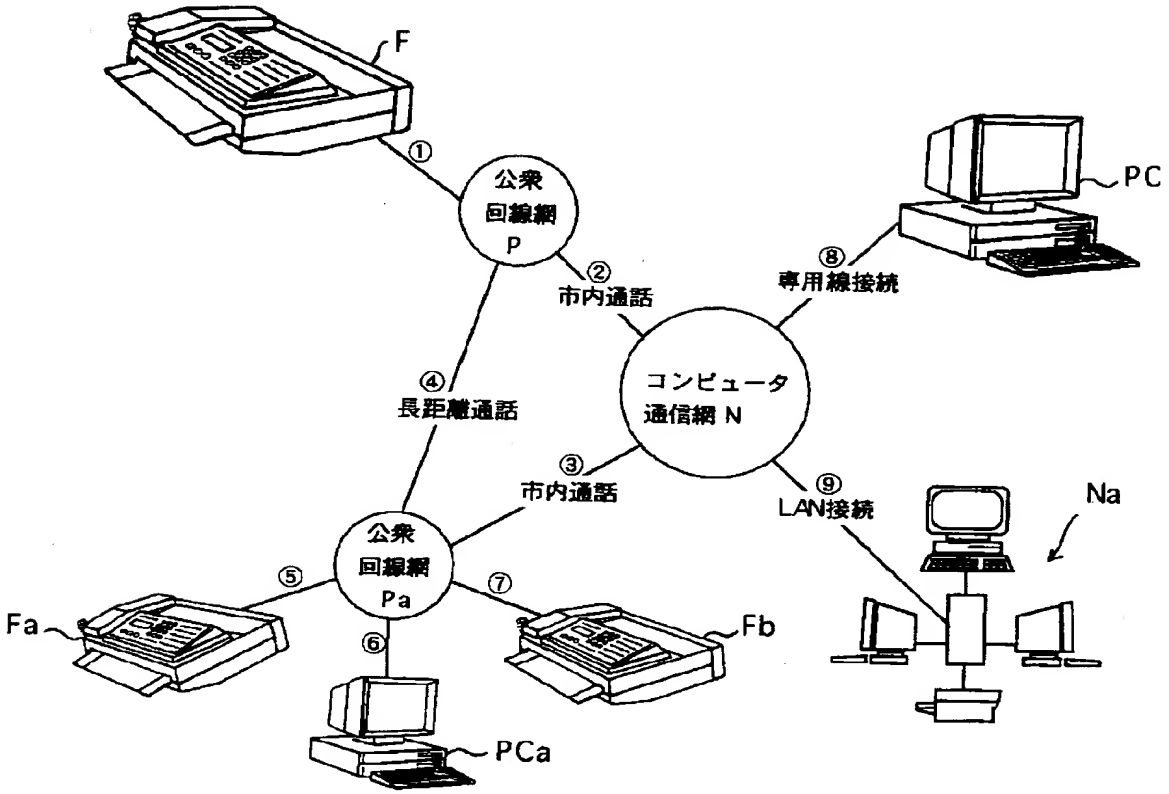
【図2】


アナログ
回線L2
NCU
11
モデム
10
オート
ダイヤラー25
デジタル
回線L1
DSU
9
利用者テーブル T1
プロバイダテーブル T2
相手先テーブル T3
(G3)
(G4)
メール
編集部24
バイナリ・テキスト
変換部23
画像
変換部22
A
符号化復号化
部21
イメージ
メモリ8
暗号部
20
読取部2
記録部3

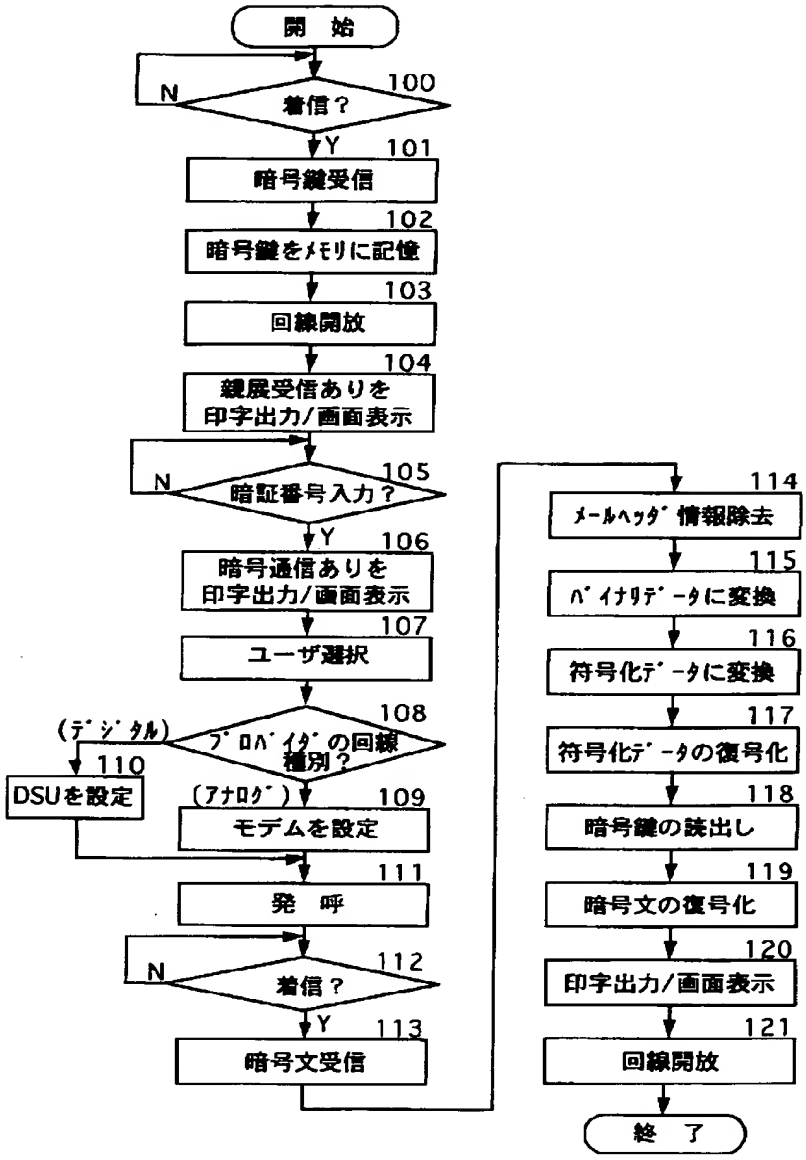
【図４】


送信側
(#01)
送信指示
(#02)
暗号化された原稿(暗号文)
をインターネットで送信
(#03)
暗号鍵を電話回線で送信
終了
受信側
(#11)
暗号鍵を電話回線から受信
(#12)
暗号化された原稿(暗号文)
をインターネットから受信
(#13)
受信原稿を暗号鍵を用いて
復号化、印刷
終了

【図5】


F
①
公衆
回線網
P
②
市内通話
④
長距離通話
コンピュータ
通信網 N
③
市内通話
⑧
専用線接続
PC
⑨
LAN接続
Na
公衆
回線網
Pa
⑤
⑦
Fa
Fb
⑥
PCa

【図６】



フロントページの続き

(51)Int.Cl.⁶	識別記号	ＦＩ	
Ｈ０４Ｍ　11/00	３０３	Ｈ０４Ｌ　11/20	１０１Ｂ
Ｈ０４Ｎ　1/44			